

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE**

NOV 04 2020

IN THE MATTER OF THE SEARCH OF:)
)
AN APPLE IPHONE S, SILVER IN)
COLOR, MODEL: A1633, CELLULAR)
TELEPHONE)
AND)
AN APPLE IPHONE, RED IN COLOR,)
CELLULAR TELEPHONE, AS FURTHER)
DESCRIBED IN ATTACHMENTS A and B)

Clk. U.S. L. Court
Eastern District of Tennessee
AT Knoxville

CASE NO. 3:20-MJ- 1170

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brandon Stryker, being duly sworn, state the following information to be true to the best of my knowledge, information and belief:

INTRODUCTION

1. I am a High Intensity Drug Trafficking Area (“HIDTA”) Task Force Officer (“TFO”) with the Federal Bureau of Investigation (“FBI”), United States Department of Justice. I have also been employed as a Police Officer with the Knoxville Police Department (“KPD”) since 2006. I have been involved in the field of law enforcement for more than fourteen years. In my current assignment as a TFO with the FBI, I am charged with the investigation of criminal conduct in violation of Title 21 of United States Code as well as related criminal acts, such as money laundering and firearms offenses. I have served as the case agent in the execution of multiple search and arrest warrants during my service and have also worked with other law enforcement officers in their investigations.

2. My experience also includes, but is not limited to, conducting physical surveillance, interviewing witnesses, writing Title III affidavits for wire intercepts, writing affidavits for and executing search warrants, working with undercover agents and informants,

issuance of administrative and federal grand jury subpoenas, analysis of phone toll and financial records, and analysis of data derived from the use of pen registers, trap and traces, and wiretaps.

3. I have received training and have experience in the investigation of violations of the federal drug and money-laundering laws. As a result, I am familiar with matters including the means and methods used by persons and drug trafficking organizations (“DTOs”) to purchase, transport, store, and distribute drugs, and to hide profits generated from those transactions. I also have experience in analyzing and interpreting drug codes and cryptic dialogue used by drug traffickers. In addition, I am also aware that it is common for members of DTOs to possess firearms in furtherance of their drug trafficking activities. In addition, it is also common to use electronic devices such as computers, cellular telephones, and other electronic means to communicate and store information relating to the DTO and the trafficking of drugs.

4. I have personally participated in the investigation of this case relating to the arrest of the defendant, Trevor Cox (“COX”), and subsequent seizure of two (2) cell phones from COX on October 15, 2020. All information within this affidavit is from my own personal participation in the investigation, during the afternoon of October 15, 2020. I am submitting this affidavit in support of an application for a warrant to search the cellular telephones collected from COX: iPhone S, silver in color, described in Attachment A (hereinafter “TARGET DEVICE 1”) and an iPhone, red in color, described in Attachment A (hereinafter “TARGET DEVICE 2”).

5. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a search warrant authorizing the search of TARGET DEVICES 1 and 2, I have not included each and every fact known to me concerning this investigation. Instead, I have

set forth only the facts that I believe are necessary to establish probable cause to believe that TARGET DEVICES 1 and 2, contain evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 846, and 841(a)(1), as further described in Attachment B.

PROBABLE CAUSE

6. On Thursday, October 8, 2020, the Federal Grand Jury of the Eastern District of Tennessee returned a second superseding federal indictment in case number 3:19-CR-151 in which COX was charged with three counts including: Conspiracy to Distribute Multiple Controlled Substances (including marijuana), Aiding and Abetting of the Possession of Firearms in Furtherance of a Drug Trafficking Crime, and Possession with Intent to Distribute Fifty (50) grams or more of Methamphetamine. Part of this investigation included a wiretap during the summer of 2019 and COX was captured on Title III wire intercepts negotiating with co-defendant Alim Turner the acquisition of more than 50 grams of methamphetamine for distribution. Additionally, a known, reliable confidential informant subsequently corroborated the fact that COX distributes controlled substances, including methamphetamine. Like many of his co-defendants in this case, COX is a confirmed member of the Vice Lords criminal street gang and has been a member for several years. Finally, Affiant's testimony to the Federal Grand Jury earlier this month resulted in the second superseding indictment, and a federal arrest warrant for COX was issued by the Court.

COX WAS ARRESTED JANUARY 31, 2017 IN KNOX COUNTY FOR POSSESSION OF MARIJUANA AND POSSESSION OF A HANDGUN WHILE UNDER THE INFLUENCE

7. On Thursday, October 15, 2020, the Affiant, along with FBI TFO Brandon Glover, observed COX driving a silver, 2016 Jeep Cherokee bearing TN registration 7C9-3S3 in the parking lot of McDonalds, located at 8451 Middlebrook Pike in Knoxville, Tennessee. The Affiant and TFO Glover had prior knowledge that COX had the aforementioned federal arrest warrants that had yet to be served. Additionally, the Affiant and TFO Glover had prior

10-23-20
BLS

knowledge that the silver 2016 Jeep Cherokee bearing TN registration 7C9-3S3 COX was driving was entered in NCIC as stolen on September 10, 2020. COX parked the vehicle at a gas pump in front of the Pilot convenience store, which is co-located with McDonalds, and exited the driver's door. Both the Affiant and TFO Glover made contact with COX and took him into custody.

8. TFO Glover then requested a marked KPD police cruiser to transport COX from the scene and for a law enforcement K-9 to respond to the scene to conduct an open-air sniff of the stolen, silver, 2016 Jeep Cherokee. COX was placed in a marked police cruiser and searched by Officer Vesser and his trainee. During the search incident to arrest, COX was found to have an iPhone S, silver in color, in his pants pocket. The iPhone S, silver in color, was powered on and had a background which stated, *"Everybody always asks where is the dopeman...but nobody ever asks How's the dopeman"* which was in plain view on the main screen of the phone (See pictures in Attachment A). "Dopeman" is a common slang term for a drug trafficker. KPD K-9 Officer Sexton later arrived with his K-9 partner to conduct an open-air sniff of the vehicle. The K-9 alerted to the odor of controlled substances emanating from within the vehicle and the vehicle was subsequently searched. During the search of the vehicle, officers located a .38 caliber revolver handgun under the driver's seat, two digital scales - one from the driver's floorboard and one from the center console, and a black vacuum-sealed bag containing marijuana residue was found in the backseat. Additionally, an iPhone, red in color, was found in the driver's door compartment. Additionally, digital scales and firearms, like the one's found in the stolen vehicle in which COX was driving, are common tools of the illegal drug trade. COX was charged with vehicle theft and possession of a firearm by a convicted felon. All of the aforementioned evidence was transported to KPD for confiscation and processing.

9. Based upon my training and experience, it is common for criminals to conceal evidence of unlawful activity within their cellular telephones. I know that criminals often utilize cellular telephones to conduct their business and plan crimes; which in this case, is engaging in drug trafficking. I am also aware that cellular telephones provide criminals with mobile access and control over their illegal trade. They often utilize cellular telephones to communicate with one another in furtherance of their unlawful activities. I know that cellular telephones frequently retain information for long periods of time, including retaining call histories, text messages, voicemail messages, photographs, internet browser history, GPS location data, and other information that can be retrieved from the cellular telephone even long after the cellular telephone ceased to be used. If unused and unaltered, most data from cellular telephones can remain indefinitely. In addition, it is common for criminals to utilize multiple cellular telephones to further their ongoing criminal activity. Criminals utilize multiple cellular telephones in their attempts to conceal their criminal activity or enterprise as a way to thwart the efforts of law enforcement. Cellular telephones are best analyzed in an offsite environment where the appropriate equipment can be used to download the data from the cellular telephone and preserve a copy of the downloaded material for inspection. Based upon my training and experience, there is probable cause to believe evidence of drug trafficking will be found on TARGET DEVICE 1 and TARGET DEVICE 2.

TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones

send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting

the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

11. Based on my training, experience, and research, I know that cellular devices such as the TARGET DEVICES, even flip phones, may have capabilities that frequently include acting as a wireless telephone, digital camera, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, evidence of a crime, or point toward the existence of evidence in other locations. This data can be evidence of a crime,

indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

12. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

13. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the particular TARGET DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the particular TARGET DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. The nature of cellular phone-related evidence requires forensic analysts to employ a variety of different techniques to search for, document, and obtain electronic evidence. The search procedure may include the following techniques (the following is a nonexclusive list, as other search procedures may be used):

i. examination of all of the data contained in the cellular telephone, and/or memory storage devices in the cellular telephone to view the data and determine whether that data falls within the items to be seized as set forth herein;

ii. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

iii. surveying various file directories and the individual files they contain;

iv. opening files in order to determine their contents;

v. scanning storage areas; and

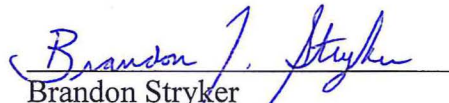
vi. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear.

14. Because this warrant seeks permission to examine only TARGET DEVICE 1 and TARGET DEVICE 2, which are already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.


CONCLUSION

15. In light of the foregoing, there is probable cause to search TARGET DEVICE 1 and TARGET DEVICE 2, as set forth in Attachment A, for evidence of drug trafficking in violation of Title 21, United States Code, Sections 846 and 841(a)(1).

Respectfully submitted,


Brandon Stryker
Task Force Officer
FBI

Subscribed and sworn to before me on this 23rd day of October, 2020.


DEBRA C. POPLIN

United States Magistrate Judge

ATTACHMENT A

TARGET DEVICE 1: Iphone S, silver in color, Model A1633 phone at arrest of Trevor COX at 8451 Middlebrook Pike, Knoxville, TN. The phone was powered on at time of seizure.



TARGET DEVICE 2: Iphone, red in color, phone at arrest of Trevor COX at 8451 Middlebrook Pike, Knoxville, TN. The phone was not powered on at time of seizure.



ATTACHMENT B

1. All records on TARGET DEVICE 1 and TARGET DEVICE 2 described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1) and 846 as follows:

- a. All communications between January 01, 2017 and October 23, 2020, in whatever form, that relate to, further in any way, or constitute evidence of drug trafficking, including all records related to those communications.
- b. All photographs, videos, audio recordings, and text messages, between January 01, 2017 and October 23, 2020, that relate to, further in any way, or constitute evidence of drug trafficking.
- c. All data, communications, information, and records, in whatever form, between January 01, 2017 and October 23, 2020, that have any tendency to establish the physical location of TARGET DEVICE 1 and TARGET DEVICE 2.
- d. All data, communications, information, and records, in whatever form, January 01, 2017 and October 23, 2020, that establish the identity or location of individuals engaged in drug trafficking.

2. Evidence of user attribution showing who used or owned the particular TARGET DEVICES at the time the electronically stored evidence described in this warrant was created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored.